BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP

TELEPHONE: (303) 740-1980

INTELLECTUAL PROPERTY LAW
12400 WILSHIRE BOULEVARD, 7TH FLOOR
LOS ANGELES, CA 90025

FACSIMILE: (303) 740-6962

RECEIVED
CENTRAL FAX CENTER
APR 25 2006

FACSIMILE COVER SHEET

Deliver to: _____ Art Group: _____

Facsimile No.: (571) 273-8300 Date: April 25, 2006

From: Libby H. Hope, Reg. No. 46,774

Our Docket No.: 42390P11149 Number of pages 29 including this sheet.

Application No.: 09/896,537 Filing Date: 6/30/2001

Docket Due Date(s): 5/1/2006

Enclosed are the following documents:

☐ Amendment: _____ (___pgs)	☐ Issue Fee Transmittal
☒ Appeal Brief (26 pgs)	☐ Notice of Appeal
☐ Application: _____	☐ Petition for: _____
(___pgs) w/cover & abstract)	☐ Request for Continued Examination (RCE)
☐ Assignment & Cover Sheet (___pgs)	☐ Reply Brief (___pgs)
☒ Certificate of Facsimile	☐ Request & Certification Under 35 USC 122(b)(2)(B)(i)
☐ Continued Prosecution Application (CPA)	☐ Request to Rescind Previous Nonpublication Request
☐ Declaration & POA (___pgs)	☐ Response to Notice of Missing Parts & Formalities Letter
☐ Drawings: ___sheets, ___ figures	☐ Response to Written Opinion (___pgs)
☐ Extension of Time: _____	☐ Terminal Disclaimer
☐ Fee Transmittal (In duplicate)	☐ Transmittal of Publication Fee Due
☐ IDS & PTO/SB/08 (pgs)	☒ Transmittal Letter
☒ Other Response to Notice of Non-Compliant Appeal Brief	

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is being transmitted by facsimile on the date shown below to the United States Patent and Trademark Office.

Libby H. Hope 4/25/2006
Date

Confidentiality Note: The documents accompanying this facsimile transmission contain information from the law firm of Blakely, Sokoloff, Taylor & Zafman which is confidential or privileged. The information is intended to be for the use of the individual or entity named on this transmission sheet. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this faxed information is prohibited. If you have received this facsimile in error, please notify us by telephone immediately so that we can arrange for the retrieval of the original documents at no cost to you.

If you do not receive all the pages, or if there is any difficulty in receiving, please call: (303) 740-1980 and ask for Libby H. Hope .

RECEIVED
CENTRAL FAX CENTER
APR 25 2006

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	28

Application No.	09/896,537
Filing Date	June 30, 2001
First Named Inventor	Gary Graunke
Art Unit	2132
Examiner Name	Lanier, Benjamin E.
Attorney Docket Number	42390P11149

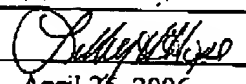
ENCLOSURES *(check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Response
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
  - ☐ PTO/SB/08
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Basic Filing Fee
  - ☐ Declaration/POA
- ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s)
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) *(please identify below):*

Certificate of Facsimile; and the Response to Notice of Non-Compliant Appeal Brief

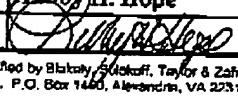
Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Libby H. Hope, Reg. No. 46,774 INTEL CORP.
Signature	
Date	April 25, 2006

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being transmitted via facsimile on the date shown below to the United States Patent and Trademark Office.

Typed or printed name	Libby H. Hope		
Signature		Date	April 25, 2006

Based on PTO/SB/21 (09-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wh) 11/30/2005.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

RECEIVED
CENTRAL FAX CENTER
APR 25 2006

Our Docket No: 42P11149

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Patent Application of: Graunke et al.	
Serial No.: 09/896,537	Examiner: Lanier, Benjamin
Assignee: Intel Corporation	
Filed: June 30, 2001	
For: MULTI-LEVEL, MULTI-DIMENSIONAL CONTENT PROTECTION	Art Unit: 2132

RESPONSE TO NOTICE OF NON-COMPLIANT APPEAL BRIEF

Mail Stop: Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

FIRST CLASS CERTIFICATE OF MAILING

I hereby certify that I am causing the above-referenced correspondence to be deposited with the United States Postal Service as first class mail with sufficient postage on the date indicated below and that this paper or fee has been addressed to the Commissioner for Patents, Alexandria, VA 22313.

Date of Deposit: April 25, 2006
Name of Person Mailing Correspondence: Libby H. Hope

Signature — April 25, 2006 Date

In response to the Notice of Non-Compliant Appeal Brief mailed on April 11, 2006, please find the amended Appeal Brief enclosed herewith to replace the Appeal Brief submitted on February 1, 2006.

Please charge any shortage to our Deposit Account No. 50-0221.

Respectfully submitted,

INTEL CORPORATION

Date: April 25, 2006

Libby H. Hope
Reg. No. 46,774

12400 Wilshire Boulevard
7th Floor
Los Angeles, California 90025-1030
(303) 740-1980

PAGE 3/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

Docket No.: 42P11149 *Utility Patent*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Patent Application of:

Graunke et al.

Serial No.: 09/896,537 Examiner: Lanier, Benjamin

Assignee: Intel Corporation

Filed: June 30, 2001

Art Unit: 2132

For: MULTI-LEVEL, MULTI-DIMENSIONAL CONTENT PROTECTION

RECEIVED
CENTRAL FAX CENTER
APR 25 2006

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 CFR §1.192
IN SUPPORT OF APPELLANTS' APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Sir:

Appellants hereby submit this Appeal Brief in support of Appellants' Appeal from final rejection of the pending claims in the above-captioned case.

A Notice of Appeal was filed on December 1, 2005.

The fees set forth in 37 CFR §1.17(c) accompany this Appeal Brief.

An oral hearing is NOT desired.

Appellants respectfully request consideration of this Appeal by the

PAGE 4/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

honorable Board of Patent Appeals and Interferences, and allowance of the claims of the subject application.

Please charge any fees and/or credit any overcharges to Deposit Account No. 50-0221.

I. REAL PARTY IN INTEREST

The subject application is assigned to Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California 95052-8119.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the current matter.

III. STATUS OF THE CLAIMS

Claims 1-28 are were rejected in the Final Office Action mailed October 7, 2005 (hereinafter "Final OA"). Claims 1-3, 11-16, and 20-22 are currently being appealed. A copy of the claims on appeal is attached hereto as Claims Appendix under section VIII.

IV. STATUS OF AMENDMENTS

An amendment to claims 12-13 and 18-19 was filed subsequent to the Final Office Action on February 1, 2006. An Advisory Action was mailed on April 11, 2006 in which these amendments were entered. The Claims Appendix lists

PAGE 5/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

all claims, including the claims as amended.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In one aspect of the invention, a method is provided for multi-level and multi-dimensional encoding of content for distribution to multiple environments. Content having one or more attributes is encrypted once and distributed to multiple environments having various levels of security. (Page 5, Paragraph 14)

Multi-dimensional encoding refers to encoding content that may have one or more attributes, such as resolution or frame-rate. Multi-level encoding refers to hierarchical encoding of content for a given attribute, where each successive level improves the attribute of the previous level, to achieve environment-independent encoding of content for one or more environments, where each environment has its own level of security. Both multi-dimensional encoding and multi-level encoding are characterized by the encoding of content once for distribution to multiple environments. (Page 5, Paragraph 15)

Multi-dimensional content is divided into sections. Each section is a portion of the content to be distributed, and represents a level of access for the attributes of the content, and each successive section is an improvement of the given attribute over the previous section. Each section is separately encrypted using separate keys from a hierarchy of keys. The keys of the hierarchy may be related by a cryptographic-strength one-way function, such that in decryption, the one-way function may be applied to any higher level section key to derive the key of the preceding, next lower level section. (Page 5, Paragraph 16)

PAGE 6/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

For a given environment, the content is conveyed such that the highest appropriate key for the attributes and assurance of the given environment are available. The lower level keys are derived using the one-way function, so that a device for accessing the content has access to all levels less than or equal to the given key, but not greater than the given key. (Page 5, Paragraph 17)

The present invention includes various operations, which will be described below. The operations of the present invention may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the operations. Alternatively, the operations may be performed by a combination of hardware and software. (Page 5-6, Paragraph 18)

The present invention may be provided as a computer program product which may include a machine-readable medium having stored thereon instructions which may be used to program a computer (or other electronic devices) to perform a process according to the present invention. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs (Compact Disc-Read Only Memories), and magneto-optical disks, ROMs (Read Only Memories), RAMs (Random Access Memories), EPROMs (Erasable Programmable Read Only Memories), EEPROMs (Electromagnetic Erasable Programmable Read Only Memories), magnetic or optical cards, flash memory, DVDs (Digital Video Discs), or other type of media / machine-readable medium suitable for storing electronic instructions. (Page 6, Paragraph 19)

PAGE 7/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

Moreover, the present invention may also be downloaded as a computer program product, wherein the program may be transferred from a remote computer (e.g., a server) to a requesting computer (e.g., a client) by way of data signals embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem or network connection). Accordingly, herein, a carrier wave shall be regarded as comprising a machine-readable medium. (Page 6, Paragraph 20)

As illustrated in FIG. 1, content 100 having a set of attributes is transformed into encrypted content 102 comprising a plurality of sections (only five sections shown) 104, 106, 108, 110, 112, where each section corresponds to one of L through N levels of access (L<N), L being the lowest level of access (e.g., lowest resolution), and N being the highest level of access (e.g., highest resolution). Each section is content encrypted at a level of access that a client may subscribe to. Encryption is achieved by using a plurality of hierarchically related keys 114, 116, 118, 120, 122, resulting in a plurality of dimensions 124 for a corresponding number of attributes. In preferred embodiments, the keys are related by a cryptographic-strength one-way function. (Page 6-7, Paragraph 21)

A method in accordance with FIG. 1 is illustrated in FIG. 4. It starts at block 400, and continues to block 402 where the hierarchical keys are generated. At block 404, encrypted content is created by applying each key to the content to create sections of the content. The method ends at block 406. (Page 7, Paragraph 22)

PAGE 8/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

As illustrated in FIG. 2, a server 200 and a client 202 create a secure authenticated channel 204 that connects a digital rights management agent 208 (hereinafter "agent") on the client with a content clearinghouse 206 (hereinafter "clearinghouse") comprising content 100 on the server 200. A request to access content 100 is received from the client 202. When the server 200 receives appropriate payment from the client 202 for an M (L<= M <= N) level of access, the encrypted content 102 is communicated to the client 202, along with the appropriate key for the level of access subscribed to. (Page 7, Paragraph 23)

As illustrated in FIG. 3, using a base key 300 (i.e., a key commensurate with the client's 202 subscription, or rights, which is K_3 in this example), the agent 208 can create all appropriate lower level keys 302, 304. Once all appropriate keys 300, 302, 304 are obtained or created, the encrypted content 102 is decrypted into accessible content 306, where the client 202 has access to the corresponding sections 308, 310, 312 (obtained by using the appropriate key 300, 302, 304) of the content 100 having the given set of attributes less than or equal to the base key 300. (Page 7, Paragraph 24)

A method in accordance with FIG. 3 is illustrated in FIG. 5, beginning at block 500. At block 502, content having N levels of access is received. At block 504, a base key corresponding to an M of N level of access is received, and at block 506, the base key is used to derive lower level keys for accessing content corresponding to those lower level keys. The method ends at block 508. (Page 7-8, Paragraph 25)

PAGE 9/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

For example, consider the case where the content's given attribute is "resolution" comprising levels of access 1-5 (i.e., L through N), where 1 is the lowest resolution and 5 is the highest resolution. If a client subscribes to a mid-point resolution, say 3 (i.e., M), then upon appropriate payment, the server transmits the content along with a base key corresponding to a resolution of 3. The client then uses the base key to generate all lower level keys. Once all appropriate keys are available, corresponding sections of the content may be accessed. (Page 8, Paragraph 26)

For synchronized, multi-media applications, synchronization information is encrypted separately from the information in each synchronized channel (for example, video and audio). That is, each aspect of the multi-media content may be separately encrypted, enabling the value of each aspect to be recognized in rights management transactions. Where various aspects interact, a multi-dimensional encryption scheme can be used wherever multi-dimensional hierarchical encoding is possible. For non-interactive aspects, each may be separately protected, or, optionally, they may be artificially related for purposes of key distribution. (Page 8, Paragraph 27)

In one exemplary embodiment, a matrix for each dimension is published, such that a key with a lower subscript in each dimension can be computed from the higher value key. In another exemplary embodiment, a modular exponentiation function is utilized. In yet another embodiment, a secret sharing scheme is utilized. (Page 8, Paragraph 28)

PAGE 10/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

In one embodiment, a random key, $K_{i,j,}$, is generated for each point on a D-dimensional grid, where D represents the number of attributes for given content. On the server side, content is encrypted into sections, or points on the grid, where each point is encrypted using its corresponding random key, $K_{i,j}$. For a dimension, X, a given matrix value in the matrix is represented by: (Page 9, Paragraph 29)

$X_{i,j} = K_{i,j} \wedge H(K_{i+1,j})$. (Page 9, Paragraph 30)

When content is transferred to the client, a base key commensurate with the client's subscription level is transmitted, along with one or more matrices, depending upon the number of attributes there are. Using the base key, a key with a lower subscript in each dimension may be computed from a higher value key. In exemplary embodiments, an exclusive-or operation may be used to derive the lower level key. For dimension X, this may be represented as follows: (Page 9, Paragraph 31)

$K_{i,j} = F_1(K,i,j) = X_{i,j} \wedge H(K_{i+1,j})$ (Page 9, Paragraph 32)

where $K_{i,j}$ represents the randomly generated key, which is derived from a higher-level key; $F_1(K,i,j)$ is the function computed by the exclusive-or of the X matrix value with the one-way function of the next highest level key $K_{i+1,j}$ in the first dimension; $X_{i,j}$ is the value at grid point (i, j) from the published matrix; and $H(K_{i+1,j})$ is a one-way function of the higher level key $K_{i+1,j}$, such as the well-known message digest function SHA-1 or MD5, for example. (Page 9, Paragraph 33)

PAGE 11/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

Similarly, for dimension Y: (Page 9, Paragraph 34)

$K_{i,j} = F_2(K,i,j) = Y_{i,j} \wedge H(K_{i,j+1})$. (Page 9, Paragraph 35)

where $K_{i,j}$ represents the randomly generated key, which is derived from a higher-level key; $F_2(K,i,j)$ is the function computed by the exclusive-or of the X matrix value with the one-way function of the next highest level key $K_{i,j+1}$ in the second dimension; $Y_{i,j}$ is the value at grid point (i, j) from the published matrix; and $H(K_{i,j+1})$ is a one-way function of the higher level key $K_{i,j+1}$, such as the well-known message digest function SHA-1 or MD5, for example. (Page 9-10, Paragraph 36)

The method can be extended to any number of dimensions. In the case of only one dimension, X can be omitted, such that: (Page 10, Paragraph 37)

$K_i = H(K_{i+1})$ (Page 10, Paragraph 38)

An example of corresponding matrices for dimensions X and Y is illustrated in FIGS. 6 and 7, where dimension X represents the attribute "frames per second", and dimension Y represents the attribute "resolution". In this example, the highest resolution and frames/second exist at grid point (3, 3). Thus, if a client subscribes to receiving the highest level of access, the environment will receive a base key corresponding to that level. (Page 10, Paragraph 39)

As illustrated at grid point (3, 3), it costs $5000 to subscribe to content having the highest level resolution and the highest level of frames per second.

PAGE 12/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

The client for an environment subscribing to these levels receives the base key, $K_{3,3}$, (all keys are the same for all dimensions). The base key, $K_{3,3}$, may then be used to generate all lower level keys. The keys may then be used to decrypt corresponding sections of the content. In progressive, hierarchical encoding, a lower level section of the content is decoded first, and each subsequent key is used to refine the previously decoded section of the content to produce a higher level attribute. (Page 10, Paragraph 40)

Using the equation for the appropriate dimension as shown above, the agent may create keys to access lower level content by computing the lower level keys based on the base key that is transmitted to the environment. (Page 10, Paragraph 41)

Keys may be generated from dimension X (FIG. 6) as follows: (Page 10, Paragraph 42)

$K_{1,1} = F_1(K,1,1) = X_{1,1} \wedge H(K_{2,1})$ (Page 11, Paragraph 43)

$K_{1,2} = F_1(K,1,2) = X_{1,2} \wedge H(K_{2,2})$ (Page 11, Paragraph 44)

$K_{2,1} = F_1(K,2,1) = X_{2,1} \wedge H(K_{3,1})$ (Page 11, Paragraph 45)

$K_{2,2} = F_1(K,2,2) = X_{2,2} \wedge H(K_{3,2})$ (Page 11, Paragraph 46)

$K_{1,3} = F_1(K,1,3) = X_{1,3} \wedge H(K_{2,3})$ (Page 11, Paragraph 47)

$K_{2,3} = F_1(K,2,3) = X_{2,3} \wedge H(K_{3,3})$ (Page 11, Paragraph 48)

Similarly, keys may be generated from dimension Y (FIG. 7) as follows:

PAGE 13/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

(Page 11, Paragraph 49)

$K_{1,1} = F_2(K,1,1) = Y_{1,1} \wedge H(K_{1,2})$ (Page 11, Paragraph 50)

$K_{1,2} = F_2(K,1,2) = Y_{1,2} \wedge H(K_{1,3})$ (Page 11, Paragraph 51)

$K_{2,1} = F_2(K,2,1) = Y_{2,1} \wedge H(K_{2,2})$ (Page 11, Paragraph 52)

$K_{2,2} = F_2(K,2,2) = Y_{2,2} \wedge H(K_{2,3})$ (Page 11, Paragraph 53)

$K_{3,1} = F_2(K,3,1) = Y_{3,1} \wedge H(K_{3,2})$ (Page 11, Paragraph 54)

$K_{3,2} = F_2(K,3,2) = Y_{3,2} \wedge H(K_{3,3})$ (Page 11, Paragraph 55)

Note that for matrix X, the rightmost entries (i.e., (3, 1) and (3, 2)) are omitted, since they are used for deriving lower-level keys to the left, and for matrix Y, the topmost entries (i.e. (1, 3) and (2,3)) are omitted, since they are used for deriving lower-level keys below. Since the keys are the same for all dimensions, entries missing from one matrix may be obtained from another matrix. Thus, equation $K_{2,2} = F_1(K,2,2) = X_{2,2} \wedge H(K_{3,2})$ from matrix X, $K_{3,2}$ may be obtained from $K_{3,2} = F_2(K,3,2) = Y_{3,2} \wedge H(K_{3,3})$ in matrix Y. (Page 11, Paragraph 56)

Using the base key and both matrices, all keys may be computed by moving to the left or moving down using an equation from a given matrix. For instance, since $K_{3,3}$ is given, $K_{3,2}$ may be computed using $K_{3,2} = F_2(K,3,2) = Y_{3,2} \wedge H(K_{3,3})$, and $K_{3,1}$ may be computed by using $K_{3,1} = F_2(K,3,1) = Y_{3,1} \wedge H(K_{3,2})$ (using "moving down" equations from matrix Y). Similarly, $K_{2,3}$ may be computed by using $K_{2,3} = F_1(K,2,3) = X_{2,3} \wedge H(K_{3,3})$, and $K_{1,3}$ may be computed by using $K_{1,3}$

PAGE 14/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

= $F_1(K,1,3) = X_{1,3} \wedge H(K_{2,3})$ (using "moving left" equations from matrix X). (Page 11-12, Paragraph 57)

$K_{2,2}$ may be computed from $K_{2,2} = F_1(K,2,2) = X_{2,2} \wedge H(K_{3,2})$ or from $K_{2,2} = F_2(K,2,2) = Y_{2,2} \wedge H(K_{2,3})$. $K_{1,2}$ may be computed from $K_{1,2} = F_1(K,1,2) = X_{1,2} \wedge H(K_{2,2})$, or from $K_{1,2} = F_2(K,1,2) = Y_{1,2} \wedge H(K_{1,3})$. $K_{2,1}$ may be computed from $K_{2,1} = F_1(K,2,1) = X_{2,1} \wedge H(K_{3,1})$ or from $K_{2,1} = F_2(K,2,1) = Y_{2,1} \wedge H(K_{2,2})$. $K_{1,1}$ may be computed from $K_{1,1} = F_1(K,1,1) = X_{1,1} \wedge H(K_{2,1})$ or from $K_{1,1} = F_2(K,1,1) = Y_{1,1} \wedge H(K_{1,2})$. (Page 12, Paragraph 58)

With this method, any path (i.e., moving left or moving down) to compute a lower value key from a higher value key produces the same result. The length of the key provided by this method is limited by the message digest that is used. For example, it would be 128 bits for MD5 and 160 bits for SHA-1. (Page 12, Paragraph 59)

In another embodiment, a public modulus, m, comprising two secret large prime factors, p and q, is selected. For each dimension, d, an exponent, e_d, relatively prime to (having no common factors with) (p-1)*(q-1) is chosen. The exponents are also pair-wise relatively prime. Since the size of the group of numbers generated is relatively large, it ensures that some approaches to inverting the modular exponentiation do not work. (Page 12, Paragraph 60)

These exponents may be small, but should be greater than 3. For the maximum value of all dimensions, i, j, ..., a secret key $K_{i,j,...}$ greater than 1 and less than m is chosen. (Page 12, Paragraph 61)

PAGE 15/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

$K_{i,j,...}$ may then be used to encrypt the content. To form the adjacent key in dimension d when decrypting, $K_{...,l,...}$, from key $K_{...,l+1...}$, raise it to the e_d power mod m. An equation for this is as follows: (Page 12-13, Paragraph 62)

$K_{...,l,...} = F_d(K_{...,i+1...}) = K_{...,l+1...}{}^{e}{}_{d} \bmod m$. (Page 13, Paragraph 63)

Assuming m is sufficiently large to disable factoring (at least 1024 bits for most applications), it would be infeasible to reverse the computation and determine higher keys in any dimension. (Page 13, Paragraph 64)

As with the first exemplary embodiment, any path to compute a lower value key from a higher value key produces the same result. This method provides up to 1024 bits for a key. (Page 13, Paragraph 65)

Consequently, the key size, size of required information, and computation requirements may help to determine which of these two methods is optimal for a given implementation. (Page 13, Paragraph 66)

In yet another embodiment, a publicly known cryptographic one-way function H, and a d-dimensional secret sharing scheme S are utilized. For dimension d, key $X_{d,l} = H(X_{d,l+1})$. Additional artificial dimensions, such as cost, may be added to provide additional constraints. Key $K_{i,j...} = S_n(X_{1,l}, X_{2,j},...)$ where S is an n-of-n secret sharing scheme. (Page 13, Paragraph 67)

For example, in FIG. 8, the client may purchase a high-resolution movie encrypted with a 2 dimensional scheme, where an artificial third dimension of cost is also added. The server would communicate shares $X_{1,3}$ and $X_{2,3}$ to the

PAGE 16/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

client. The client would compute lesser value shares in each dimension using the hash function H as follows: (Page 13, Paragraph 68)

$X_{1,2} = H(X_{1,3})$, $X_{1,1} = H(X_{1,2})$ (Page 13, Paragraph 69)

$X_{2,2} = H(X_{2,3})$, $X_{2,1} = H(X_{2,2})$, and (Page 13, Paragraph 70)

$X_{3,5} = H(X_{3,6})$, $X_{3,4} = H(X_{3,5})$, $X_{3,3} = H(X_{3,4})$, $X_{3,3} = H(X_{3,4})$, $X_{3,2} = H(X_{3,3})$, $X_{3,1} = H(X_{3,2})$. (Page 13-14, Paragraph 71)

The client may then compute all the particular shares, $K_{i,j}$, used to decrypt the various portions of hierarchically encrypted and encoded content using a 3-of-3 secret sharing scheme S: (Page 14, Paragraph 72)

$K_{1,3} = S_3(X_{1,1}, X_{2,3,}, X_{3,3})$, $K_{2,3} = S_3(X_{1,2}, X_{2,3,}, X_{3,5})$, $K_{3,3} = S_3(X_{1,3}, X_{2,3,}, X_{3,6})$; (Page 14, Paragraph 73)

$K_{1,2} = S_3(X_{1,1}, X_{2,2,}, X_{3,2})$, $K_{2,2} = S_3(X_{1,2}, X_{2,2,}, X_{3,4})$, $K_{3,2} = S_3(X_{1,3}, X_{2,2,}, X_{3,5})$; (Page 14, Paragraph 74)

$K_{1,1} = S_3(X_{1,1}, X_{2,1,}, X_{3,1})$, $K_{2,1} = S_3(X_{1,2}, X_{2,1,}, X_{3,2})$, $K_{3,1} = S_3(X_{1,3}, X_{2,1,}, X_{3,3})$; (Page 14, Paragraph 75)

giving it access to all encrypted portions of the content. (Page 14, Paragraph 76)

The additional artificial cost dimension prevents one from purchasing both $K_{1,3}$ and $K_{3,1}$, obtaining both $X_{2,3}$ and $X_{1,3}$ and being able to construct $K_{3,3}$ or $K_{2,2}$. In this case, the artificial dimension reflects the additional value of the integration

PAGE 17/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

of the dimensions. (Page 14, Paragraph 77)

Once all appropriate keys have been generated, content may be accessed by applying a key to its corresponding section. In an exemplary embodiment, lower level sections of the content are decoded first, and each successive section is decoded to refine the previously decoded section. (Page 14, Paragraph 78)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 2, 11-12, 14, 15, 20, and 21 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,485,577 ("Eyer").

Claims 3, 13, 16, and 22 stand rejected under 35 U.S.C. §103(a) as being obvious over Eyer and U.S. Patent No. 5,448,639 ("Arazi").

VII. ARGUMENT

REJECTION UNDER 35 U.S.C. §102(b) OVER U.S. PATENT NO. 5,485,577 (HEREINAFTER "EYER")

Claims 1, 2, 11-12, 14, 15, 20, and 21

As the Honorable Board is well aware, a "claim is anticipated only if *each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference*." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Applicants respectfully submit that claims 1, 2, 11-12, 14, 15, 20, and 21 are patentably distinguishable over Eyer. At the least, Eyer does not disclose

PAGE 18/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

"content comprising a set of attributes having L through N levels of access", as required by, for example, claim 1. Each of the other remaining pending independent claims recite limitations that are similar to these limitations of claim 1, although some differences may exist among the limitations of the other pending independent claims. These similar limitations nevertheless patentably distinguish the claims over Eyer.

Eyer discloses a method for incrementally delivering authenticated access rights to an access control processor. In Eyer, data defining the access rights is divided into a plurality of subgroups which are transmitted to the processor as authenticated data in a plurality of messages. Upon receipt of a message by the processor, a current cryptographic key is derived using the authenticated data of the current message. The current cryptographic key is compared to a cryptographic key from a prior message. If the keys match, then the validity designation for that key is set to a valid state for each storage bank that is storing data authenticated by the current message. If the keys do not match, the validity designation for that key is set to a valid state for each storage bank that is storing data authenticated by the current message, and the validity designation for that keys is set to an invalid state for all other storage banks. (Eyer, column 2, lines 19-41.)

In embodiments of the claimed invention, content may comprise a set of attributes. For example, an attribute may comprise "resolution". Furthermore, the attributes may have L through N levels of access. For resolution, for example, 1 may be the lowest resolution that may be accessed (e.g., subscribed

PAGE 19/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

to), and 5 may be the highest resolution that may be accessed (e.g., subscribed to). See further, for example, Specification at paragraphs 21, 23, and 26.

In response, the Examiner asserts that "Eyer discloses that the television signals have subscription and premium services (Col. 1, lines 14-30), which would correspond to the different levels of access. For example the base level of access would be your run of the mill basic cable, and the maximum level of access, which correspond to N of the claims, would be access to all channels that the television provider has available. Element M of the claims would correspond to some point in between, which could be basic cable plus HBO for example. These levels of access are represented in the access rights that the terminals receive and furthermore in the decryption keys that are later generated from those access rights. Therefore Eyer discloses the "levels of access" as claimed." (Final OA, page 2, Item 1).

Applicants respectfully disagree. The claims of the subject application clearly require receiving "content comprising a set of *attributes having L through N levels of access*" (emphasis added). While Eyer discloses data that may be divided into a plurality of subgroups, Eyer does not disclose that such data has attributes which have levels of access as required by the claimed invention.

Thus, since Eyer does not teach or disclose each and every element of the claimed invention, it is respectfully submitted that the Examiner has failed to establish prima facie that claims 1, 2, 11-12, 14, 15, 20, and 21 are anticipated by Eyer. Thus, it is respectfully submitted that the Examiner's rejection of these claims under 35 U.S.C. §102(b) as being anticipated by Eyer is erroneous, and

PAGE 20/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

respectfully requested that the Examiner's rejection of these claims be reversed.

REJECTION UNDER 35 U.S.C §103(a) OVER U.S. PATENT NO. 5,485,577 ("EYER") AND U.S. PATENT NO. 5,448,639 ("Arazi")

Claims 3, 13, 16, and 22

As the Honorable Board is well aware, in order to establish a *prima facie* case of obviousness:

First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations." (Emphasis added). *In re Vaech*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Manual of Patent Examining Procedure (MPEP), 8th Edition, August 2001, §2143.

Applicants respectfully submit that the Examiner has not established a prima facie case of obviousness because:

1. There is no suggestion or motivation in Eyer or in Arazi for combination.
2. The combination of Eyer and Arazi does not teach or suggest all the claim limitations.

PAGE 21/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

There is no suggestion or motivation in Eyer or in Arazi for combination

The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). MPEP §2143.01. Furthermore, though a combined element may be a "technologically simple concept", the reference must still provide the motivation for the combination. (*In re Kotzah*, 217 F.3d at 1371, 55 USPQ2d at 1318.) MPEP §2143.01.

Arazi discloses a digital signature device that comprises hardware or software means for carrying out modular exponentiation and/or modular multiplication operations. (Arazi, column 1, lines 47-50.)

While Eyer is directed to incremental delivery of access rights to data, Arazi is directed to a digital signature device. The fact that Eyer may use digital signatures, however, does not make it a candidate for combination with Arazi absent a suggestion for desirability of the combination. Applicants submit that such suggestion is absent because the references address different needs. Eyer addresses a need for a secure method for transmission of data, while Arazi addresses a need for a simplified and less expensive digital signature device. Applicants respectfully submit that the combination of Eyer with Arazi is not suggested in either reference.

In response to this, the Examiner indicates that "it would have been obvious to one of ordinary skill in the art at the time the invention was made to

PAGE 22/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

generate the cryptographic keys of Eyer using the modular exponentiation methods of Arazi in order to reduce overhead as disclosed in Arazi" (Final OA, page 2-3).

However, as the Manual of Patent Examining Procedure (MPEP), §2142 indicates, the "initial burden is on the examiner to provide some suggestion of the desirability of doing what the inventor has done. 'To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teaching of the references.' *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Intef. 1985). Applicants respectfully submit that the Examiner has failed to meet this burden, and maintain that both Eyer and Arazi lack the suggestion or motivation for combination.

The combination of Eyer and Arazi does not teach or suggest all the claim limitations

As discussed above, Eyer does not disclose "content comprising a set of attributes having L through N levels of access", as required by, for example, claim 1. Furthermore, Arazi does not disclose, teach, or suggest that which Eyer is missing. Therefore, the combination of Eyer and Arazi does not teach or suggest all the claim limitations, and therefore does not produce the Applicants' invention as embodied in the claims.

PAGE 23/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

Since the Examiner has not established a prima facie case of obviousness, the combination of Eyer and Arazi is in error. Thus, it is respectfully requested that the Examiner's rejection of claims 3, 3, 16, and 22 under 35 U.S.C. §103(a) as obvious in view of Eyer and Arazi be withdrawn.

VIII. CLAIMS APPENDIX

1. A method comprising:

receiving content comprising a set of attributes having L through N levels of access, where L<N, and content at a given level of access being decryptable by a corresponding key;

receiving a base key corresponding to an M of N level of access, where L<=M<=N; and

deriving lower level keys based on the base key, the lower level keys being used to access content having an M level of access or lower.

2. The method of claim 1, additionally comprising receiving a D-dimensional matrix for each attribute in the set of attributes, wherein D corresponds to a number of attributes of the content, and wherein the matrix comprises matrix values for determining how to generate a key corresponding to a given section of the content, and said deriving lower level keys based on the base key comprises, for a given lower level key, using a function based on a matrix value corresponding to the lower level key and a one-way hash function of an adjacent higher level key.

PAGE 24/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

3. The method of claim 1, wherein said deriving lower level keys based on the base key comprises, for a given lower level key, using a modular exponentiation of a higher level key.

11. A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following:

receive content comprising a set of attributes having L through N levels of access, where L<N, and content at a given level of access being decryptable by a corresponding key;

receive a base key corresponding to an M of N level of access, where L<=M<=N; and

derive lower level keys based on the base key, the lower level keys being used to access content having an M level of access of lower.

12. The machine-readable medium of claim 11, additionally comprising instructions that cause the processor to receive a D-dimensional matrix for each attribute in the set of attributes, wherein D corresponds to a number of attributes of the content, and wherein the matrix comprises matrix values for determining how to generate a key corresponding to a given section of the content, and the instructions cause the processor to derive lower level keys based on the base key comprises, for a given lower level key, using a function based on a matrix value corresponding to the lower

PAGE 25/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

level key and a one-way function of an adjacent higher level key.

13. The machine-readable medium of claim 11, wherein the instructions cause the processor to derive lower level keys based on the base key comprises, for a given lower level key, by using a modular exponentiation of a higher level key.

14. An apparatus comprising:

at least one processor; and

a machine-readable medium having instructions encoded thereon, which when executed by the processor, are capable of directing the processor to:

receive content comprising a set of attributes having L through N levels of access, where L<N, and content at a given level of access being decryptable by a corresponding key;

receive a base key corresponding to an M of N level of access, where L<=M<=N; and

derive lower level keys based on the base key, the lower level keys being used to access content having an M level of access of lower.

15. The apparatus of claim 14, additionally comprising instructions that cause the processor to receive a D-dimensional matrix for each attribute in the

PAGE 26/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

set of attributes, wherein D corresponds to a number of attributes of the content, and wherein the matrix comprises matrix values for determining how to generate a key corresponding to a given section of the content, and the instructions cause the processor to derive lower level keys based on the base key comprises, for a given lower level key, using a function based on a matrix value corresponding to the lower level key and a one-way hash function of an adjacent higher level key.

16. The apparatus of claim 14, wherein the instructions cause the processor to derive lower level keys based on the base key comprises, for a given lower level key, by using a modular exponentiation of a higher level key.

20. A method comprising:

receiving encrypted content comprising a set of attributes having L through N levels of access, where L<N, and each level being accessible by a corresponding key;

receiving a base key corresponding to an M of N level of access, where L<=M<=N;

deriving lower level keys based on the base key, the lower level keys being used to access content having an M level of access or lower; and

using a given lower level key to decrypt the content at a corresponding level.

PAGE 27/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

21. The method of claim 20, additionally comprising receiving a D-dimensional matrix for each attribute in the set of attributes, wherein D corresponds to a number of attributes of the content, and wherein the matrix comprises matrix values for determining how to generate a key corresponding to a given section of the content, and said deriving lower level keys based on the base key comprises, for a given lower level key, using a function based on a matrix value corresponding to the lower level key and a one-way function of an adjacent higher level key.

22. The method of claim 20, wherein said deriving lower level keys based on the base key comprises, for a given lower level key, using a modular exponentiation of a higher level key.

IX. EVIDENCE APPENDIX

Applicants are not relying on in this Appeal, and therefore not submitting, any evidence pursuant to CFR (Code of Federal Regulations) Title 37, §§ 1.130, 1.131, or 1.132.

X. RELATED PROCEEDINGS APPENDIX

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the current matter. Therefore, no decisions are submitted in this appendix.

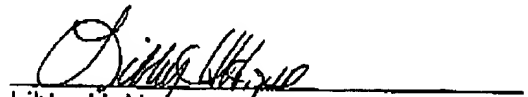
PAGE 28/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56

CONCLUSION

For the reasons discussed above, Appellants respectfully submit that each and every one of the final rejections made by the Examiner in the Final Office Action is erroneous. Accordingly, Appellants respectfully request that the Honorable Board of Patent Appeals and Interferences reverse the Examiner and direct that all of the currently pending claims be allowed.

Respectfully submitted,

Date: April 25, 2006



Libby H. Hope
Attorney for Appellants
Reg. No. 46,774
Patent Practice Group
INTEL CORPORATION

PAGE 29/29 * RCVD AT 4/25/2006 7:28:05 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:9494980601 * DURATION (mm-ss):06-56